

Securities and Exchange Commission

Office of Inspector General

During the first half of fiscal year 2007, the Office of Inspector General assisted the Commission in its efforts to:

- Complete required staff performance management steps throughout the Commission in a timely and appropriate fashion,
- Improve the process for providing staff interpretative guidance in the Full Disclosure Program,
- Implement procedures to resolve backlogs of Freedom of Information Act requests and comment letter postings to the Internet,
- Enhance the integrity of the Commission and its staff by investigating allegations of misconduct,
- Improve information technology security for the Blue Sheets and Super Tracking and Reporting systems,
- Enhance the management of information technology within the Division of Enforcement,
- Ensure appropriate use and security of the Name Relationship Search Index system, and
- Further the implementation of the Commission's risk assessment function.

Executive Summary

During this period (October 1, 2006 to March 31, 2007), the Office of Inspector General (Office) issued four audit reports, two evaluation reports, and one investigative memorandum on management issues, and completed one survey.

These evaluations focused on management of staff performance in the Division of Enforcement; information technology (IT) management in the Division of Enforcement; Full Disclosure interpretive guidance; security evaluations of the Blue Sheets and Super Tracking and Reporting (STARS) systems; a backlog of requests under the Freedom of Information Act (FOIA); training and guidance for the Name Relationship Search Inquiry (NRSI) system; and the Office of Risk Assessment. This work is described in more detail in the Audit Program section below.

Five investigations were closed during the period.¹ Three subjects were referred to the Department of Justice, which declined prosecution. Five subjects were referred to Commission management. Two of these subjects (both contractor employees) resigned. Two other subjects were reprimanded and one was counseled. In addition, two subjects referred during prior semi-annual periods were suspended, and one subject referred during the prior period was reprimanded. Two subjects referred during prior semi-annual periods are awaiting disposition. The Investigative Program section below describes the significant cases closed during the period.

We are adding a new significant problem, removing one previously reported significant problem, and retaining another previously reported significant problem.

We are reporting the Commission's management of staff performance as a new significant problem, based on our review of the Division of Enforcement's staff performance management. In that review, we found that Enforcement did not consistently perform parts of the performance evaluation process and did not retain performance documentation for the required amount of time. The Executive Director indicated that the current Commission-wide staff performance management system needs improvement. The Commission plans to change its process to address deficiencies in the current system and to better ensure that required steps of the process are followed.

In its 2006 audit of the Commission's financial statements, the Government Accountability Office found no material weaknesses. Based on their findings, we are removing financial management systems controls as a significant problem.

Our Office has reported information technology (IT) management as a significant problem for several years. During that time, the Office of Information Technology has taken numerous steps to improve IT management. Although it remains a significant problem at

¹ Two investigations closed during the prior semi-annual period (April 1, 2006 to September 30, 2006) were inadvertently omitted from the semi-annual report for the second half of fiscal year 2006. A subject of one of these investigations was referred to the Department of Justice, which declined prosecution.

this time, we have begun a special project to evaluate whether these steps, taken as a whole, have corrected this significant problem.

No management decisions were revised during the period. The Office of Inspector General agrees with all significant management decisions regarding audit recommendations.

Audit Program

During this period, the Office issued four audit reports, two evaluation reports, and one investigative memorandum on management issues. The Office also completed a survey.

These evaluations are summarized below. Management generally concurred with our recommendations, and in many cases took corrective actions during the evaluations. A list of pending evaluations follows the summaries.

IT MANAGEMENT IN ENFORCEMENT (NO. 405)

Our review of the Division of Enforcement's IT management found that it was generally adequate. However, the Division needs to issue additional guidance to ensure a sound IT program. We recommended that the Division prepare an IT plan and document its procedures for IT management, major initiatives (such as the document imaging project), and security management.

During our review, the Division and the Office of Administrative Services (OAS) developed procedures for preventing and resolving physical security incidents at the Division's forensics lab.

FULL DISCLOSURE INTERPRETATIVE GUIDANCE (NO. 416)

We reviewed the process for issuing staff interpretive guidance for the Full Disclosure program. The Division of Corporation Finance and the Office of the Chief Accountant have primary responsibility for issuing this guidance.

We identified a number of possible improvements to the process. Our recommendations concern Staff Accounting Bulletins; disclosure of staff guidance; workload, timeliness, and reporting issues; file documentation; and procedures for responding to guidance requests and approving speeches.

SYSTEMS SECURITY EVALUATION—BLUE SHEETS (NO. 417)

We issued a task order to Electronic Consulting Services, Inc. (ECS) to evaluate the security of the Blue Sheets system under the Federal Information Security Management Act (FISMA). The evaluation found that the Commission significantly improved its

certification and accreditation process in fiscal year 2006 by remedying four of the five weaknesses we identified during our fiscal year 2005 FISMA evaluation.

We identified no high risk vulnerabilities and nine medium risk vulnerabilities. The medium risk vulnerabilities concerned the risk assessment report; vulnerability scanning; the system security plan; system documentation; external interconnections; the plan of action and milestones; the disaster recovery plan; baseline configuration and inventory; and configuration change control.

Our overall FISMA evaluation report for fiscal year 2006 contained recommendations to address most of these vulnerabilities. We made additional recommendations, as appropriate, in this report. The Office of Information Technology agrees with the findings and is performing an analysis on how to best implement the recommendations.

OFFICE OF RISK ASSESSMENT (NO. 420)

We surveyed the Office of Risk Assessment (ORA), which was created several years ago to enhance the Commission's risk assessment function. During the survey, we gathered background information about ORA and its activities for audit planning purposes.

Because of the limited objective and scope of our survey, we did not issue a written report or make any recommendations. We discussed several issues with ORA management, including the definition of its mission and its resource needs.

FOIA BACKLOG (NO. 422)

The Divisions of Corporation Finance and Investment Management issue comment letters on filings they receive. Over the last several years, commercial users significantly increased their Freedom of Information Act (FOIA) requests for these comment letters. These requests created a large backlog, which we analyzed in this audit.

Besides the influx of requests, we identified several other factors which helped cause the backlog. These included: management's decision to post a large number of already issued letters on the Commission website, which created a separate backlog of letters to be posted; inefficient processing procedures; and limited staff.

We made several recommendations to the two Divisions and the Commission's FOIA Office to improve the efficiency of processing procedures, both for FOIA requests and the posting of letters on the website. The Divisions and the FOIA Office have taken and plan to take several steps to address the FOIA backlog.

ENFORCEMENT PERFORMANCE MANAGEMENT (NO. 423)

We reviewed the Division of Enforcement's compliance with required performance management procedures. We found that the Division did not consistently perform parts of the performance appraisal process, especially for new, reassigned and detailed staff. Many Enforcement managers were not comfortable giving unacceptable ratings to poor

performers and did not consistently retain performance documentation for the required time. We also found that the Office of Human Resources (OHR) guidance to Commission managers needed improvement.

We recommended that the Division ensure its supervisors perform all required performance management steps and that the OHR improve its written guidance and provide additional training.

Enforcement management suggested that our findings were typical of the Commission as a whole. The Commission's Executive Director indicated that the current performance management program needs significant improvements. Starting in fiscal year 2008, the Commission will adopt a new program to address the deficiencies.

Because the Commission-wide staff performance management system is ineffective, we consider it to be a significant problem (see below).

SYSTEMS SECURITY EVALUATION—STARS (NO. 424)

In addition to the Blue Sheets security evaluation (see above), we issued a task order to Electronic Consulting Services, Inc. (ECS) to evaluate the security of the Super Tracking and Reporting System (STARS).

We identified one high risk deficiency (a significant vulnerability requiring immediate action) within STARS: the need to encrypt data while in transit. We also found eight medium risk vulnerabilities (significant deficiencies requiring timely action).

The medium risk vulnerabilities concerned the STARS security categorization; the risk assessment report; the system security plan; system documentation; the plan of action and milestones; the disaster recovery plan; baseline configuration and inventory; and configuration change control. As appropriate, we made recommendations to address these vulnerabilities. The Office of Information Technology agrees with the findings and is performing an analysis on how to best implement the recommendations.

NRSI TRAINING AND WARNING (NOS. G-442/433)

Commission staff use the Name Relationship Search Index (NRSI) system to research all of the relationships that companies or individuals have had with the Commission. During two Office investigations (OIG-442 and OIG-433), we identified a need to improve user training on NRSI to help prevent inappropriate use of the system. We also found that the warning on the NRSI login screen does not inform employees that the NRSI database is to be used only for official purposes.

We recommended improving NRSI training and appropriately modifying the warning on the NRSI login screen.

PENDING EVALUATIONS

The following evaluations were pending at the close of the semi-annual period (March 31, 2007):

No. 421 Investment Company Filing Initiatives

No. 427 DynCorp Contract—Detailed Review

No. 428 Document Imaging

No. 429 XBRL Survey

No. 430 Contract Ratifications

No. 431 IT Management Significant Problem

No. 432 Receiver Oversight

Investigative Program

Five investigations were closed during the period. Three subjects were referred to the Department of Justice, which declined prosecution. Five subjects were referred to Commission management. Two of these subjects (both contractor employees) resigned. Two other subjects were reprimanded and one was counseled. In addition, two subjects referred during prior semi-annual periods were suspended, and one subject referred during the prior period was reprimanded. Two subjects referred during prior semi-annual periods are awaiting disposition.

The most significant cases closed during the period, as well as a case closed during the prior period,² are described below.

THEFT OF GOVERNMENT INFORMATION

An Office investigation developed evidence that an employee who left the Commission took large quantities of non-public Commission information and loaded it onto his new employer's computer system. The non-public Commission information was returned, and the Department of Justice declined prosecution.

CONTRACTOR FRAUD

The Office investigated allegations that a Commission contractor was billing for non-existent employees, billing more than once for the same work, and offering bonuses to staff to take longer to complete work. The evidence developed during the investigation failed to substantiate the allegations.

² As mentioned in footnote 1 above, two cases closed during the prior semi-annual period were inadvertently omitted from our last semi-annual report.

MISUSE OF DATABASE

An Office investigation disclosed that a staff member had searched a non-public Commission database for information unrelated to the employee's job responsibilities. We found no evidence, however, that the employee had released non-public information to unauthorized persons. Management counseled the employee about proper use of the database.

FAILURE TO REPORT SECURITIES TRANSACTIONS

The Office investigated an allegation that a staff member had used his position at the Commission to assist a relative with selling securities. Our investigation disclosed no evidence of misuse of position to assist the relative. However, we did find evidence that the employee failed to report investments as required by a Commission rule, failed to consider the potential for the appearance of a conflict of interest, and exhibited a possible lack of candor. The employee was reprimanded and required to attend ethics counseling and training.

MISUSE OF COMPUTER RESOURCES AND FALSE STATEMENTS

An Office investigation developed evidence that three contractor employees had misused Commission computer resources to support a personal computer business. We also found evidence that the employees made false statements about these activities, and that one of the employees had previously lied to the agency about his arrest record. Our investigation did not find evidence that the employees had sold any used Commission hardware or software through their computer business, and the Department of Justice declined prosecution. Two of the employees resigned, and the contractor reprimanded the third employee.

Significant Problems

STAFF PERFORMANCE MANAGEMENT

This period, the Office identified a significant problem with the Commission's staff performance management system, based on audit work conducted in the Division of Enforcement (see Audit No. 423 above).

Although the audit scope was limited to the Division of Enforcement, the Executive Director agreed that the Commission-wide staff performance management program needs significant improvement. The Commission plans to adopt a new performance management program to address the deficiencies, starting in fiscal year 2008.

Because the Commission-wide staff performance management system is ineffective, we consider it to be a significant problem.

Significant Problems Identified Previously

FINANCIAL MANAGEMENT SYSTEMS CONTROLS

An OIG contractor completed an audit of Commission financial management systems controls during a prior period (Audit No. 362). The audit found that Commission financial management controls for fiscal year 2002 were effective in all material respects, based on criteria established under the Federal Managers Financial Integrity Act, except for three material weaknesses and one material non-conformance.

The exceptions concerned property accountability, accounting and control of disgorgements, information system and security program controls, and the Disgorgement and Penalties Tracking System. We reported that, taken together, these financial management exceptions were a significant problem for the Commission. Management concurred with our recommendations to strengthen these financial controls, and promptly began to take actions to correct the weaknesses.

The Government Accountability Office (GAO) performed the audit of the Commission's financial statements for fiscal years 2004 and 2005. The audits found that the Commission has made significant progress in building a financial reporting structure for preparing financial statements for audit.

GAO also found that the SEC property account balance was below the threshold for materiality; as a consequence we had previously removed property accountability as an element of this significant problem. However, GAO identified material internal control weaknesses in preparing financial statements and related disclosures, recording and reporting disgorgements and penalties, and information security, which became the basis for this significant problem.

During its audit of the Commission's fiscal year 2006 financial statements, GAO indicated that it no longer considers the weaknesses in financial reporting, disgorgements and penalties, and information security to be material, based on the corrective actions taken by the Commission. Accordingly, we are removing financial management systems controls as a significant problem.

INFORMATION TECHNOLOGY MANAGEMENT

Since April 1996, we have reported information technology (IT) management as a significant problem based on weaknesses identified by several audits, investigations, and management studies. Significant IT management weaknesses included information

systems security; IT capital investment decision-making; administration of IT contracts; IT project management; enterprise architecture management; strategic management of IT human capital; and management of software licenses.

We no longer consider information systems security to be an element of this significant problem, based on our fiscal year 2006 FISMA evaluation and GAO's audit of the Commission's fiscal year 2006 financial statements. The Office of Information Technology (OIT) indicated that it has continued to strengthen IT management during this reporting period and expects it will no longer be a significant problem by the end of fiscal year 2007.

We have begun a special project to evaluate whether the progress made by OIT in strengthening IT management is sufficient to warrant removing it as a significant problem.

Access to Information

The Office of Inspector General has received access to all information required to carry out its activities. No reports to the Chairman, concerning refusal of such information, were made during the period.

Other Matters

EXTERNAL COORDINATION

The Office actively participates in the activities of the Executive Council on Integrity and Efficiency (ECIE). The Inspector General attends ECIE meetings, is an active member of its Financial Institutions Regulatory Committee, and serves as the ECIE member on the Integrity Committee (established by Executive Order No. 12993).

The Deputy Inspector General is an active member of the Federal Audit Executive Council (FAEC). The FAEC considers audit issues relevant to the Inspector General community.

The Counsel to the Inspector General is the Vice-Chair of the PCIE Council of Counsels; the Associate Counsel is an active member. The Council considers legal issues relevant to the Inspector General community.

REVIEW OF LEGISLATION AND REGULATIONS

The Office reviewed legislation and proposed and final rules relating to the programs and operations of the Commission, pursuant to the Inspector General Act. We tracked both legislation and regulations by researching relevant documents and databases, including lists prepared by the IG community and the Commission's Office of General Counsel. Our independent assessments focused on the impact of the legislation or rule on the economy and efficiency of, and the prevention and detection of fraud and abuse in, programs and

operations administered by the Commission. In addition, we reviewed statutes and regulations within the context of audits and investigations (*e.g.*, the impact of the Federal Information Security Management Act on Commission operations).

In conjunction with the Legislation Committee of the PCIE/ECIE, we also reviewed legislation and rules that would have an impact on the Inspector General community. We provided comments to the PCIE Legislation Committee on the “Accountability in Government Contracting Act of 2007.”

Questioned Costs

		DOLLAR VALUE (IN THOUSANDS)		
		<u>NUMBER</u>	<u>UNSUPPORTED COSTS</u>	<u>QUESTIONED COSTS</u>
A	For which no management decision has been made by the commencement of the reporting period	0	0	0
B	<i>Which were issued during the reporting period</i>	<u>0</u>	<u>0</u>	<u>0</u>
	Subtotals (A+B)	0	0	0
C	For which a management decision was made during the reporting period	0	0	0
(i)	Dollar value of disallowed costs	0	0	0
(ii)	Dollar value of costs not disallowed	0	0	0
D	For which no management decision has been made by the end of the period	0	0	0
	Reports for which no management decision was made within six months of issuance	0	0	0

Recommendations That Funds Be Put To Better Use

		<u>NUMBER</u>	<u>DOLLAR VALUE (IN THOUSANDS)</u>
A	For which no management decision has been made by the commencement of the reporting period	0	0
B	Which were issued during the reporting period	<u>0</u>	<u>0</u>
	-		
	Subtotals (A+B)	0	0
C	For which a management decision was made during the period	0	0
	(i) Dollar value of recommendations that were agreed to by management	0	0
	- Based on proposed management action	0	0
	- Based on proposed legislative action	0	0
	(ii) Dollar value of recommendations that were not agreed to by management	0	0
D	For which no management decision has been made by the end of the reporting period	0	0
	Reports for which no management decision was made within six months of issuance	0	0

Reports with No Management Decisions

Management decisions have been made on all audit reports issued before the beginning of this reporting period (October 1, 2006).

Revised Management Decisions

No management decisions were revised during the period.

Agreement with Significant Management Decisions

The Office of Inspector General agrees with all significant management decisions regarding audit recommendations.